

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-188906

(43)Date of publication of application : 04.07.2003

(51)Int.Cl.

H04L 12/56

(21)Application number : 2001-385202

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 18.12.2001

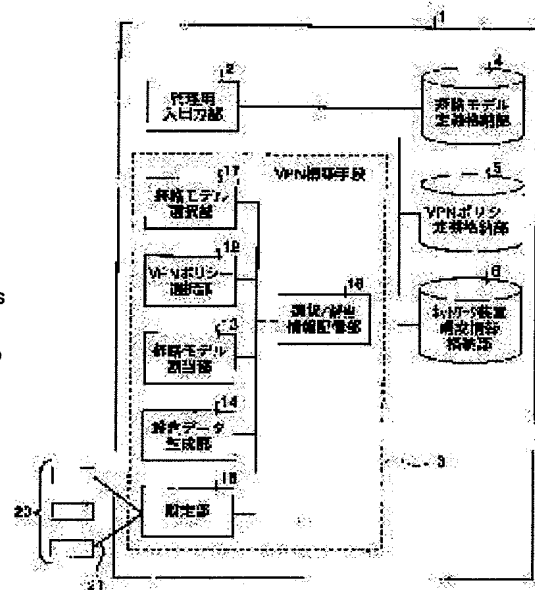
(72)Inventor : SAKAMOTO YUKO
HARADA MICHIAKI
TAKANO HIROSHI
KANAEGAMI ATSUSHI

(54) VPN POLYCY MANAGEMENT DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a VPN policy management device that can easily generate set data to a plurality of devices existing on a set route in an attempt of constructing a VPN.

SOLUTION: This VPN policy management device is provided with a route model composed of a plurality of rolls expressed by functions required for constructing the VPN, a VPN policy generated correspondingly to the route model and containing another roll in part defined to each roll constituting the route model as a parameter, and configuration information containing the address information on the devices existing on the set route. This management device is also provided with a VPN constructing means 3 which assigns the rolls of the route model to the devices existing on the set route when the end roll of the route model is assigned to two end points on the set route and, at the same time, sets set data to each device by generating the set data by substituting the address information on the devices corresponding to another roll extracted from the configurational information into the VPN policy using the another roll as a parameter.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-188906
(P2003-188906A)

(43) 公開日 平成15年7月4日 (2003.7.4)

(51) Int.Cl.⁷

H 0 4 L 12/56

識別記号

1 0 0

4 0 0

F I

H 0 4 L 12/56

テーマコード(参考)

1 0 0 C 5 K 0 3 0

4 0 0 A

審査請求 未請求 請求項の数 3 O L (全 17 頁)

(21) 出願番号 特願2001-385202(P2001-385202)

(22) 出願日 平成13年12月18日 (2001.12.18)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 坂本 優子

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 原田 道明

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100089118

弁理士 酒井 宏明

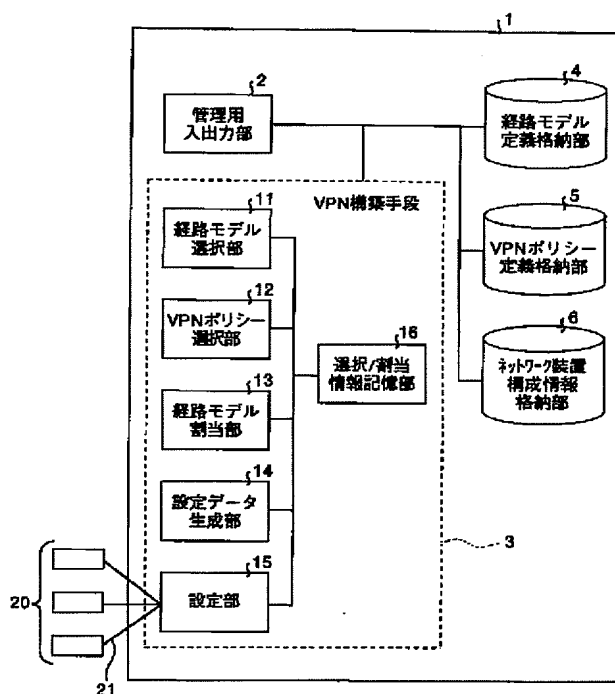
最終頁に続く

(54) 【発明の名称】 VPNポリシー管理装置

(57) 【要約】

【課題】 VPNを構築しようとしている設定経路上の複数の装置に対する設定データを容易に生成することができるVPNポリシー管理装置を得ること。

【解決手段】 VPNを構築するために必要な機能で表現した複数のロールからなる経路モデルと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むVPNポリシーと、前記設定経路上に存在する装置についてのアドレス情報を含む構成情報と、前記設定経路上の二つのエンドポイントに、前記経路モデルのエンドロールが割当てられると、前記経路モデルのロールを前記設定経路上の装置に割当てるとともに、他のロールをパラメータとして使用しているVPNポリシーに、前記構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成し、該設定データを各装置に設定するVPN構築手段3を備える。



【特許請求の範囲】

【請求項 1】 インターネットを介して接続される二つのエンドポイント間の通信経路上に VPN を構築するための VPN ポリシー管理装置であって、VPN を構築するために必要な機能で表現した複数のロールからなる経路モデルと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含む VPN ポリシーと、前記設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報と、前記設定経路上の二つのエンドポイントに、前記経路モデルの終端部を定義するエンドロールが割当てられると、前記経路モデルのロールを前記設定経路上の装置に割当てるとともに、前記 VPN ポリシーの中で他のロールをパラメータとして使用している VPN ポリシーに、前記構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成し、該設定データを前記設定経路上の各装置に設定する VPN 構築手段と、を備えることを特徴とする VPN ポリシー管理装置。

【請求項 2】 VPN を構築するために必要な機能で表現した複数のロールからなる経路モデルを格納している経路モデル定義データベースと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含む VPN ポリシーを格納している VPN ポリシー定義データベースと、VPN を構築しようとするインターネットを介して接続される二つのエンドポイント間の設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報を有するネットワーク装置構成情報データベースと、前記設定経路と適合する経路モデルが前記経路モデル定義データベースから選択される経路モデル選択手段と、前記経路モデルが選択されると、該経路モデルに対応する VPN ポリシーが前記 VPN ポリシー定義データベースから選択される VPN ポリシー選択手段と、前記設定経路中に存在する装置またはセグメントをノードとし、前記エンドポイントへ向かう方向に該ノードに隣接して接続されるセグメントまたは装置を子ノードとして幅優先で配置し、同じノードが二度以上出現した場合であって、同じ経路に出現したときには該ノードは配置せずにそこでノードの展開処理を終了し、別の経路に出現したときには該ノードを配置してそこでノードの展開処理を終了し、前記設定経路中のインターネットをルートノードとしてこれらのノードを階層化して配置したツリー構造を前記構成情報に基づいて生成するツリー構造生成機能と、前記エンドポイントに対応するノードに

前記経路モデルの終端部を定義するエンドロールが割当てられると、前記経路モデルを満たす前記ノード間の前記ツリー構造上における一以上の経路を抽出し、該一以上の経路の中から前記経路モデルを満たすノードの配置関係を有する一の経路が選択されるとともに、該経路上の装置に前記経路モデルのロールを割当てるロール割当機能と、を含む経路モデル割当手段と、前記経路上の装置にロールが割当てられると、前記 VPN ポリシーの中で他のロールをパラメータとして使用している VPN ポリシーに、前記ネットワーク装置構成情報データベースに格納されている構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成する設定データ生成手段と、該生成された設定データを前記設定経路上の装置に設定する設定手段と、を備えることを特徴とする VPN ポリシー管理装置。

【請求項 3】 前記経路モデルは、ロールごとに、該ロールが必要とする機能条件、前記設定経路上での位置が規定される構成条件、および前記ロールが前記経路モデル中で必要とされる数が定義されていることを特徴とする請求項 1 または 2 に記載の VPN ポリシー管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、IP ネットワーク上における端末間の通信を VPN (Virtual Private Network) で行う際に、VPN の構築および周辺装置の動作設定を簡易に行うことが可能な VPN ポリシー管理装置に関するものである。

【0002】

【従来の技術】VPN (Virtual Private Network) は、インターネットなどの信頼性の低いネットワークを介したプロジェクトメンバ間の通信において通信データを暗号化し、プロジェクトメンバ以外のユーザに対して通信を解読させないようにすることで、プロジェクトメンバだけの仮想的な専用線を提供するシステムである。図 17 は、複数拠点に分散したプロジェクトメンバのために構築した VPN を示す図である。図 17 の 500 ~ 502 はプロジェクトメンバが分散している距離の離れたサイトを、510 ~ 515 はそれぞれのサイトに存在するプロジェクトメンバが利用するホストを、520 ~ 522 はそれぞれのサイトに存在する VPN 装置を、530 ~ 532 はそれぞれのサイト 500 ~ 502 に存在する VPN 装置 520 ~ 522 間の VPN をそれぞれ表わしている。サイト 500 ~ 502 間はインターネットなどの外部ネットワークで接続されている。

【0003】サイト 500 ~ 502 間において、VPN 530 ~ 532 を利用せずに、そのまま外部ネットワークを利用すると外部ネットワーク上の他のユーザにサイト 500 ~ 502 間の通信データを盗聴される恐れがある。そのためサイト 500 ~ 502 間の通信を、VPN

装置 520～522 を用いて暗号化することで、VPN（仮想専用線）530～532 を提供することができる。VPN 装置 520～522 は各サイト 500～502 の入り口に存在し、あるサイトのホストが他のサイトのホストと通信する際、あるホストと同じサイト上の VPN 装置が通信データを暗号化した後に外部ネットワークにデータを出力し、このデータを相手サイトの VPN 装置が受け取り復号化した後、発信先のホストに平文（暗号化していないデータ）のデータを送付する。このような VPN を構築するためには、図 17 の VPN 装置 520～522 間に対して暗号通信を行うためのトンネルを定義しなければならない。トンネルの定義は両端の VPN 装置 520～522 に対して設定され、例えば、図 17 の VPN 装置 520 には、二つのトンネルすなわち VPN 530、531 に関する設定が行われる。

【0004】また、VPN を定義するには、VPN 装置 520～522 の設定だけでなく通信の経路上にある図示しない複数種類の装置の設定も行わなければならない場合がある。図 18 は、サイト内にファイアウォール装置を備える場合の VPN の構成を模式的に示す図である。この図 18 のサイト 550 において、551 は VPN 装置、552 はファイアウォール装置である。このように VPN 装置 551 の外側にファイアウォール装置 552 が設置されている場合、該ファイアウォール装置 552 のパケットフィルタリング機能に対して暗号化されたパケットを通過させる設定を行わなければならない。またファイアウォール装置 552 がアドレス変換を行っている場合、暗号化プロトコルの種類によっては暗号化されたパケットのポート番号が変わると正しく処理できない場合があるので、暗号化されたパケットのポート番号を変更しないように設定を行う必要がある。

【0005】図 19 は、VPN 機能を持ったモバイル端末を用いて自宅等のサイト外からサイト内に接続するリモートアクセス VPN の構成を模式的に示す図である。ここで、560 はサイトを、561 はサイト 560 の VPN 装置を示している。562 はリモートアクセスサーバであり、リモートアクセスによる接続をサイト 560 内に接続する役割を有する。そして、564 はインターネットアクセスプロバイダのアクセスポイントを示している。

【0006】このようなリモートアクセス VPN では、組織の建屋内からのアクセスであることが保証されているサイト間 VPN と異なり、モバイル端末からアクセスしてきたユーザが本当にそのプロジェクトのメンバーであるかどうかを確認するためにリモートアクセスサーバではユーザ認証と呼ばれるプロセスを実行する。このため、リモートアクセス VPN では、接続を許されたユーザのリストや各ユーザの接続先、使用可能なサービスなどについての設定も必要となる。また、リモートアクセス VPN の中でも、アクセスサーバの設置方法には様々

な形態があるので、通信経路上に必要とされる装置がそれらの形態によって異なるものとなる。

【0007】このように、VPN の設定では、設定経路上に存在する複数種類の装置の設定を行わなくてはならず、また VPN を構築する対象ネットワークの形態によって設定対象装置が異なる。すなわち、設定対象ネットワークの個々の装置に対してそれぞれ VPN の設定を行わなければならない。

【0008】しかし、IETF（Internet Engineering Task Force）のポリシーフレームワーキンググループが開発した PCIM（Policy Core Information Model）および PCIMe（Policy Core Information Model Extensions）では、装置に対してロール（役割）を割付け、ロールに対してポリシーを定義することを可能とした。ここで、ポリシーとは、ネットワークを構成する装置に対する設定を簡易にするための方法の一つであり、設定データを装置ベンダ固有の形式に依存しない抽象化されたデータ構造で記述するものである。これらの方法を用いることで、すべての装置に対して別々にポリシーを定義することが避けられ、ポリシー定義の作業効率が向上した。

【0009】

【発明が解決しようとする課題】しかしながら、これらの PCIM や PCIMe を用いた方法では、VPN 経路上の複数の装置の相互動作を考慮した上で設定を行わなければならない点は従来と同様であり、VPN 経路上の装置の設定は VPN ポリシー管理者の作業を煩雑にするものであるという問題点があった。

【0010】この発明は、上記に鑑みてなされたもので、VPN を構築しようとしている設定経路上に存在する複数の装置に対する VPN の設定データを容易に生成することができる VPN ポリシー管理装置を得ることを目的とする。

【0011】

【課題を解決するための手段】上記目的を達成するため、この発明にかかる VPN ポリシー管理装置は、VPN を構築するために必要な機能で表現した複数のロールからなる経路モデルと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含む VPN ポリシーと、前記設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報と、前記設定経路上の二つのエンドポイントに、前記経路モデルの終端部を定義するエンドロールが割当てられると、前記経路モデルのロールを前記設定経路上の装置に割当てるとともに、前記 VPN ポリシーの中で他のロールをパラメータとして使用している VPN ポリシーに、前記構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成し、該設定データを前記設定経路上の各装

置に設定するVPN構築手段と、を備えることを特徴とする。

【0012】この発明によれば、インターネットを介して接続される設定経路上の二つのエンドポイント間にVPNを構築するためのVPNポリシー管理装置が提供される。該VPNポリシー管理装置には、VPNを構築するために必要な機能で表現した複数のロールからなる経路モデルと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むVPNポリシーと、前記設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報とが格納されている。そして、VPN構築手段によって、前記設定経路上の二つのエンドポイントに、前記経路モデルの終端部を定義するエンドロールが割当てられると、前記経路モデルのロールが前記設定経路上の装置に割当てられる。また、前記VPNポリシーの中で他のロールをパラメータとして使用しているVPNポリシーに、前記構成情報から抽出された前記他のロールに対応する装置のアドレス情報が代入され、設定データが生成される。そして、該設定データが前記設定経路上の各装置に設定される。

【0013】つぎの発明にかかるVPNポリシー管理装置は、VPNを構築するために必要な機能で表現した複数のロールからなる経路モデルを格納している経路モデル定義データベースと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むVPNポリシーを格納しているVPNポリシー定義データベースと、VPNを構築しようとするインターネットを介して接続される二つのエンドポイント間の設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報を有するネットワーク装置構成情報データベースと、前記設定経路と適合する経路モデルが前記経路モデル定義データベースから選択される経路モデル選択手段と、前記経路モデルが選択されると、該経路モデルに対応するVPNポリシーが前記VPNポリシー定義データベースから選択されるVPNポリシー選択手段と、前記設定経路中に存在する装置またはセグメントをノードとし、前記エンドポイントへ向かう方向に該ノードに隣接して接続されるセグメントまたは装置を子ノードとして幅優先で配置し、同じノードが二度以上出現した場合であって、同じ経路に出現したときには該ノードは配置せずにそこでノードの展開処理を終了し、別の経路に出現したときには該ノードを配置してそこでノードの展開処理を終了し、前記設定経路中のインターネットをルートノードとしてこれらのノードを階層化して配置したツリー構造を前記構成情報に基づいて生成するツリー構造生成機能と、前記エンドポイントに対応するノードに前記経路モデルの終端部

を定義するエンドロールが割当てられると、前記経路モデルを満たす前記ノード間の前記ツリー構造上における一以上の経路を抽出し、該一以上の経路の中から前記経路モデルを満たすノードの配置関係を有する一の経路が選択されるとともに、該経路上の装置に前記経路モデルのロールを割当てるロール割当機能と、を含む経路モデル割当手段と、前記経路上の装置にロールが割当てられると、前記VPNポリシーの中で他のロールをパラメータとして使用しているVPNポリシーに、前記ネットワーク装置構成情報データベースに格納されている構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データを生成する設定データ生成手段と、該生成された設定データを前記設定経路上の装置に設定する設定手段と、を備えることを特徴とする。

【0014】この発明によれば、インターネットを介して接続される二つのエンドポイント間の通信経路上にVPNを構築するためのVPNポリシー管理装置が提供される。経路モデル定義データベースによって、VPNを構築するために必要な機能で表現した複数のロールからなる経路モデルが格納される。また、VPNポリシー定義データベースによって、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含むVPNポリシーが格納される。そして、ネットワーク装置構成情報データベースによって、VPNを構築しようとするインターネットを介して接続される二つのエンドポイント間の設定経路上に存在する装置についての機能、アドレス情報、および設定経路上での装置間の配置関係を含む構成情報が格納される。

【0015】まず、経路モデル選択手段のツリー構造生成手段によって、前記設定経路と適合する経路モデルが前記経路モデル定義データベースから選択される。つぎに、VPNポリシー選択手段によって、前記経路モデルが選択されると、該経路モデルに対応するVPNポリシーが前記VPNポリシー定義データベースから選択される。そして、経路モデル割当手段のツリー構造生成機能によって、前記設定経路中に存在する装置またはセグメントがノードとされ、前記エンドポイントへ向かう方向に該ノードに隣接して接続されるセグメントまたは装置が子ノードとして幅優先で配置される。この際、同じノードが二度以上出現した場合であって、同じ経路に出現したときには該ノードは配置されずにそこでノードの展開処理が終了され、別の経路に出現したときには該ノードが配置されてそこでノードの展開処理が終了される。また、前記設定経路中のインターネットをルートノードとしてこれらのノードを階層化して配置したツリー構造が前記構成情報に基づいて生成される。

【0016】また、経路モデル選択手段のロール割当機能によって、前記エンドポイントに対応するノードに前記経路モデルの終端部を定義するエンドロールが割当て

られると、前記経路モデルを満たす前記ノード間の前記ツリー構造上における一以上の経路が抽出され、該一以上の経路の中から前記経路モデルを満たすノードの配置関係を有する一の経路が選択されるとともに、該経路上の装置に前記経路モデルのロールが割当てられる。

【0017】つぎに、設定データ生成手段によって、前記経路上の装置にロールが割当てられると、前記VPNポリシーの中で他のロールをパラメータとして使用しているVPNポリシーに、前記ネットワーク装置構成情報データベースに格納されている構成情報から抽出した前記他のロールに対応する装置のアドレス情報を代入して設定データが生成される。そして、設定手段によって、該生成された設定データが前記設定経路上の装置に設定される。

【0018】つぎの発明にかかるVPNポリシー管理装置は、上記の発明において、前記経路モデルは、ロールごとに、該ロールが必要とする機能条件、前記設定経路上での位置が規定される構成条件、および前記ロールが前記経路モデル中で必要とされる数が定義されていることを特徴とする。

【0019】この発明によれば、ロールごとに、該ロールが必要とする機能条件、前記設定経路上での位置が規定される構成条件、および前記ロールが前記経路モデル中で必要とされる数が前記経路モデルに定義される。この経路モデルによって、VPN経路を構築するにあたって必要な装置の情報が、機能や構成で表現される。

【0020】

【発明の実施の形態】以下に、添付図面を参照して、この発明にかかるVPNポリシー管理装置の好適な実施の形態について詳細に説明する。

【0021】実施の形態1. 図1は、この発明にかかるVPNポリシー管理装置の実施の形態1を示すブロック図である。VPNポリシー管理装置1は、管理用入出力部2と、VPN構築手段3と、経路モデル定義格納部4と、VPNポリシー定義格納部5と、ネットワーク装置構成情報格納部6とを備えている。VPN構築手段3は、さらに、経路モデル選択部11と、VPNポリシー選択部12と、経路モデル割当部13と、設定データ生成部14と、設定部15と、選択／割当情報記憶部16とを含む構成となっている。また、設定部15はVPN経路上の各装置20とネットワークなどの接続線21を介して接続されている。

【0022】管理用入出力部2によって、ポリシー設計者が経路モデルやVPNポリシーの定義を行い、そしてVPN管理者がネットワークを構成する装置の構成情報やVPNの設定を行う。経路モデル定義格納部4には、ポリシー設計者によって定義された経路モデルが格納される。VPNポリシー定義格納部5には、ポリシー設計者によって定義されたVPNポリシーが格納される。ここで、VPNポリシー定義格納部5に格納されているV

PNポリシーは、経路モデル定義格納部4に格納されている経路モデルのいずれかと関連付けされている。また、一つの経路モデルに対するVPNポリシーは複数定義することも可能である。ネットワーク装置構成情報格納部6には、VPN管理者によって予めネットワークを構成する装置の構成情報が格納されている。VPN構築手段3は、VPN管理者がVPNを構築するための手段であり、詳細についてはVPNポリシー管理装置の動作処理手順の箇所後述する。

【0023】最初に、この発明で重要な役割を果たす経路モデルについて説明する。図2は、経路モデル定義格納部4に格納される定義された経路モデルの一例を示す図である。経路モデルとは、VPNの経路上に存在する設定対象装置の列を、役割（以下、ロールという）の順序列として抽象化して表現したものである。より詳しくは、設定対象となるネットワーク上の装置列を、具体的な装置名で定義するのではなく、要求される機能すなわちロールという形で順序化して表現したものである。この経路モデルは、VPNの形態別に定義される。そして、経路モデルの各ロールには、各ロールが実際の装置に割当てるために必要な適用条件が定義されている。

【0024】例えば、図2に示される経路モデルは、サイト間VPNを定義するものであり、この経路モデルを定義する適用条件の項目として、「ロール名」、「機能条件」、「構成条件」、「最小数」および「最大数」が設定されている。

【0025】ここで、「ロール名」は、経路モデル中でロールを一意に識別するための名称である。また、「機能条件」は、装置に各ロールを割当てるときに装置が持つべき機能に関する条件である。

【0026】「構成条件」は、装置に各ロールを割当てるときに、その装置が他のロールとの位置関係において満たすべき条件である。この構成条件は、例えば一つの経路内におけるインターネットなどの信頼できないネットワークからの距離によって表現される。図2では、不等号を用いて距離の大小を表し、不等号の小さい方がよりインターネットに近いことを表している。また、この構成条件において、表中のある行はその行より上位の行で定義済みのロールとの関係で位置が決められるようになっている。ここで、構成条件の不等号にイコール

(=)が含まれている場合には、その両側のロールが同一装置に割当てられてもよいことを示している。

【0027】「最小数」は、そのロールを割当てるときに装置数の最小数である。この値が0である場合には、VPNを構築するにあたりそのロールに対応する装置は必ずしも存在する必要はないことを意味している。また、「最大数」は、そのロールを割当てるときに装置数の最大数である。ネットワーク上では異なる目的で設置された装置であってもVPNにとって同じ役割を持つ場合には、それら複数の装置に対して同じロールが割当てられる。

【0028】つぎに、この図2に示されたサイト間VPNの経路モデルを構成する各ロールについて説明する。

【0029】最初に、ロール名「第一エンド」、「第二エンド」について説明する。「第一エンド」、「第二エンド」というロールは通信の両端のエンドポイントを指すものである。機能条件として、「送受信機能」と定義されているが、エンドポイントに配置される装置として送受信機能を有することが必要なことを示している。エンドポイントは最優先に決められるべきロールであるため、構成条件はエンドポイントに対しては存在しない。したがって、図2中ではなんの条件も定義されていない。また、エンドポイントは必須の構成要件であるために、最小数は「1」と定義されている。最大数については、エンドポイントはグループであってもよいので、図2中では最大数が複数と設定されている。

【0030】つぎに、ロール名「第一VPN」、「第二VPN」について説明する。「第一VPN」、「第二VPN」というロールは、VPNのトンネルの端点となるVPN装置を表わすものである。このロールに対する機能条件として、IPsec機能を有すること、そして、構成条件として、インターネットとエンドノード（エンドポイントを構成する機器）との中間に位置することが定義されている。この構成条件中で、第一VPNと第一エンドの位置関係にイコール（=）が含まれているのは、第一エンドを割当てられたノードがIPsec機能を持つ場合、このノードにさらに、第一VPNのロールを割当て、該ノードが二つのロールを有してもよいことを意味している。第二VPNと第二エンドとの関係も同様である。また、最小数、最大数ともに「1」であるので、第一VPNおよび第二VPNはそれぞれ一台必要である。

【0031】同様に、「第一外部ファイアウォール（図中では「第一外部FW」と表記する）」、「第二外部ファイアウォール（図中では「第二外部FW」と表記する）」というロールは、機能条件として、パケットフィルタリング（PF）機能を有し、構成条件として、第一VPNまたは第二VPNよりも外側でインターネットよりも内側に位置する装置であり、この経路モデルでは無くてもよいし、複数設けてもよいことを表している。また、「第一内部ファイアウォール（図中では「第一内部FW」と表記する）」、「第二内部ファイアウォール（図中では「第二内部FW」と表記する）」というロールは、機能条件として、パケットフィルタリング（PF）機能を有し、構成条件として、第一VPNまたは第二VPNよりも内側で第一エンドポイントまたは第二エンドポイントよりも外側に位置する装置であり、この経路モデルでは無くてもよいし、複数設けてもよいことを表している。

【0032】なお、上述した構成条件の説明において、「内側」および「外側」という表現は、各エンドポイン

トからインターネットへ向かう方向を「外側」と定義したときの相対的な位置関係を表している。

【0033】上述した経路モデルの構成条件に示されたインターネットとの位置関係から、第一エンド、第一VPN、第一外部ファイアウォールおよび第一内部ファイアウォールが一つのサイトに存在すること、第二エンド、第二VPN、第二外部ファイアウォールおよび第二内部ファイアウォールが別の一つのサイトに存在することが表されている。

10 【0034】つぎに、上述した経路モデルとともに、この発明で重要な役割を果たすVPNポリシーについて説明する。図3および図4は、VPNポリシー定義格納部5に格納される定義されたVPNポリシーの一例であって、図2に示された経路モデル定義に対して作成されたVPNポリシー定義を示す図である。すなわち、図2の経路モデルに関連付けられて作成されたVPNポリシーを示す図である。

20 【0035】この図3および図4に例示されるVPNポリシーは、プロジェクトにおけるプロジェクトサーバとプロジェクトに所属する端末との間のポリシーを定義した「プロジェクトサーバポリシー」である。このVPNポリシーには、プロジェクトに所属する端末からプロジェクトサーバへのtelnet（テルネット）接続を暗号化通信により行うための規則が定義されている。

30 【0036】図2の経路モデルを構成するロールのうちこのVPNポリシーにおいて設定対象となるロール名は、第一VPN、第一外部ファイアウォール、第一内部ファイアウォール、第二VPN、第二外部ファイアウォールおよび第二内部ファイアウォールである。したがって、この図3および図4に示されるVPNポリシーの例ではこれらの各ロールに対するポリシーが定義されている。

40 【0037】このVPNポリシーの中で、「設定先ロール」には上記した設定対象となるロール名が格納される。この「設定先ロール」に対するVPNポリシーとして「規則」が設けられる。VPNポリシーは、「規則」の集合として定義されるので、一つのVPNポリシーに対して複数規則が存在することもある。この「規則」は、発信元、発信先、サービスなどの設定項目を含む「条件」と、アクション、対向装置、割当などの設定項目を含む「アクション」との組み合わせとして記述される。そのため、図3および図4では、「規則」は「条件」と「アクション」のさらに細かな項目からなる。ポリシー設定者がこれらを記述することによって、「設定先ロール」が「条件」を満たす場合には「アクション」が実行される、という形式のVPNポリシーが定義される。

50 【0038】つぎに、各設定先ロールに定義される規則の内容について説明する。まず、「設定先ロール」がVPNの場合、「規則」の「条件」は、方向、発信元（S

rc) アドレス、発信先 (Dst) アドレス、サービス (Service) などからなる。方向は、エンドポイントからインターネットに向かう方向を外側と定義した場合の該ルールに対応する装置を通過する情報の向きを定めるものである。例えば、エンドポイントからインターネットへ向かう場合には“out”、逆の場合には“in”となる。発信元アドレスと発信先アドレスは、コンピュータやサブネット、ユーザなど、通信を自発的に送受信するエンドポイントを定める。また、サービスは、プロトコルやTCP/UDP (Transmission Control Protocol/User Datagram Protocol) のポート番号、ICMP (Internet Control Message Protocol) のタイプやコードによって識別されるIPネットワーク上の通信アプリケーションを指定するものである。

【0039】一方、「規則」の「アクション」は、アクション (Action)、対向装置、割当 (Proposal) などからなる。アクションは発信元アドレス、発信先アドレス、サービスで定義される「条件」に一致したパケットを受信した装置が行うべき動作を定義するものである。対向装置は、該ルールを割当てられたVPN装置と対になるVPN装置を定めるものである。また、割当は、暗号のアルゴリズムとしてどの方法を用いるのかなどの定義を定めるものである。なお、ルール「VPN」に定義されるアクションには、つぎの三種の種類が存在する。

(1) 通過：受信したパケットをそのまま送信する。

(2) 廃棄：受信したパケットを廃棄する。

(3) 暗号化：受信したパケットを指定された方法で暗号化または復号（暗号を解く）した後送信する。暗号化の場合は暗号化の方法もアクションの一部として定義される。

【0040】つぎに、「設定先ルール」がファイアウォールの場合、「規則」の「条件」は、方向、発信元アドレス、発信先アドレス、サービスからなり、これらに記述する内容はVPNの場合と同様である。一方の「アクション」は、アクションのみである。このアクションは、VPNの場合と異なり、通過と廃棄の二種類となるが、これらに記述する内容はVPNと同様である。

【0041】「設定先ルール」がアドレス変換 (NAT) 装置の場合、「規則」の「条件」は、方向、発信元アドレス、発信先アドレス、サービスからなり、これらに記述する内容はVPNの場合と同様である。一方の「アクション」は、アクションのみである。このアクションに記述する内容は、VPNやファイアウォールの場合とは異なり、つぎのようになる。

(1) 変換：受信したパケットのIPアドレス等を変換した後送信する。変換の場合は変換方法も定義される。

(2) 無変換：受信したパケットをそのまま送信する。

【0042】このようにして、経路モデルの各ルールに対してVPNポリシーが記述される。例えば、図3にお

ける「設定先ルール」が第一VPNであるポリシーには二つの規則が規定されており、そのうちの一つの「条件」は「方向=out; Src=第一エンド; Dst=第二エンド; Service=telnet」であり、この条件に対する「アクション」は「Action=暗号; 対向装置=第二VPN; Proposal=ABC」となっている。ここで、条件の「方向=out」は第一エンドから第一VPNの外側に送信される通信を意味している。そして、「Src=第一エンド」は発信元IPアドレスが第一エンドで指定される装置であることを、「Dst=第二エンド」は発信先IPアドレスが第二エンドで指定される装置であることを示している。また、「Service=telnet」はサービスとしてtelnet接続を使用する場合を定めている。一方、アクションの「Action=暗号」は上記の「条件」を満たす場合の通信は暗号化することを示している。「対向装置=第二VPN」は暗号化された通信の送られる装置が第二VPNで定義されている装置であることを示している。そして、「Proposal=ABC」は暗号化のアルゴリズムとして“ABC”という名称のアルゴリズムを割当てて示している。

【0043】すなわち、「発信元アドレスとして第一エンドを、発信先アドレスとして第二エンドを有し、telnet接続して第一VPNを外側に向かって流れる情報であるならば、“ABC”という暗号化方法によって該情報を暗号化して第二VPNまで送信する」ことを定義している。

【0044】図3および図4中において、枠線で囲まれている表示部分が、経路モデル内のルールを用いたパラメータである。これらの経路モデルへのVPNポリシーにおいては、発信元IPアドレスなど具体的な装置が決まらなと入力できない値を経路モデル内のルールをパラメータとして表現できることを特徴とする。すなわち、経路モデルに対するVPNポリシーは、経路モデルに含まれる各ルールに対して、経路モデルに含まれる自分および他のルールをパラメータとして用いることを許されたVPNポリシー定義方法によって作成される。したがって、経路モデル中の各ルールは、それぞれ関連付けされたポリシーによって構成されている。

【0045】つぎに、この発明にかかるVPNポリシー管理装置1を用いたVPNポリシー管理方法について説明する。ただし、以下に説明するVPNポリシー管理方法において、ポリシー設計者によって予め経路モデル定義格納部4に経路モデルが、また、VPNポリシー定義格納部5にVPNポリシーが、それぞれ既に格納されている場合を前提とする。

【0046】また、VPNを構築したいと考えている実際のネットワーク（以下、実ネットワークという）上の設定経路として、VPN管理者は図5に示される経路を考えているものとする。この図5において、実ネットワ

ーク 100 はサイト A とサイト B とがインターネットを介して接続されている。サイト A 内にサーバ A 101、ホスト B 102 および VPN 装置 C 103 が存在し、VPN 装置 C 103 はサイト A とインターネットとの境界に配置されている。また、サイト B 内には、ファイアウォール装置 D (図中では「FW 装置 D」と表記する) 104、VPN 装置 E 105、ホスト F 106、ホスト G 107 およびホスト H 108 が存在しサイト B とインターネットとの境界にファイアウォール装置 D 104 が配置されている。なお、この発明において、セグメントとは、直結関係を含めたすべての装置間接続のことをいうものとする。

【0047】図 6 は、図 5 に示される実ネットワーク上の装置の構成情報である。また、この図 6 に示される構成情報は、ネットワーク装置構成情報格納部 6 に格納されているデータの形態でもある。この図に示されるように、構成情報は、装置名、IP アドレス、機能を含む情報である。「装置名」には、実ネットワーク上の装置名が格納されており、「IP アドレス」は該装置の IP アドレスが、そして「機能」には該装置の有する機能が格納されている。

【0048】ここで、図 5 および図 6 から、サイト A では、VPN 装置 C 103 がパケットフィルタリング機能と IPsec 機能とを有している。また、サイト B では、サイト B とインターネットとの入り口にあるファイアウォール装置 D 104 がパケットフィルタリング機能を有し、それよりも内側に位置する VPN 装置 E 105 が IPsec 機能を有している。

【0049】この図 5 に示される実ネットワーク 100 において、サイト A とサイト B にまたがったプロジェクトが存在し、サイト A のサーバ A 101 がプロジェクトサーバで、サイト B のホスト F 106 およびホスト G 107 がプロジェクトに参加する端末であり、サーバ A 101 と、ホスト F 106 およびホスト G 107 からなるグループ (以下、グループ FG という) 109 との間に VPN を張る場合の VPN ポリシーの処理手順について説明する。

【0050】図 7 は、VPN ポリシー管理装置の動作処理手順を示すフローチャートである。まず、VPN 管理者は、実ネットワーク上で、VPN を構築したい端末間の経路を抽出する。ここでは、サーバ A 401 とグループ FG 410 間が、VPN を構築したい端末間の経路である。VPN ポリシー管理装置 1 の経路モデル選択部 11 は、管理用入出力部 2 を介して VPN 管理者に対して、経路モデル定義格納部 4 に格納されている経路モデルを表示する (ステップ S 1)。VPN 管理者は、表示された経路モデルの中から、抽出した実ネットワークの経路と合致すると思われる経路モデルを管理用入出力部 2 から入力する。経路モデル選択部 11 は、VPN 管理者によって入力された経路モデルを経路モデル定義格納

部 4 より選択し、選択/割当情報記憶部 16 に格納する (ステップ S 2)。ここで、VPN 管理者が、図 2 に示される経路モデルを選択したものとする。図 8 は、この図 2 に対応する経路モデルのロール列を示す図である。

【0051】つぎに、VPN ポリシー選択部 12 は、選択/割当情報記憶部 16 に格納された経路モデルと関連付けされた VPN ポリシーを VPN ポリシー定義格納部 5 より抽出し、管理用入出力部 2 を介して VPN 管理者に対して表示する (ステップ S 3)。VPN 管理者は、表示された VPN ポリシーの中からさらに構築しようとしている VPN に適当な VPN ポリシーを管理用入出力部 2 から選択する。VPN ポリシー選択部 12 は、VPN 管理者によって入力された VPN ポリシーを VPN ポリシー定義格納部 5 より選択し、選択/割当情報記憶部 16 に格納する (ステップ S 4)。ここで、VPN 管理者は、図 3 に示される VPN ポリシーを選択したものとする。

【0052】VPN 管理者は、管理用入出力部 2 から、選択した経路モデル中のエンドポイントの二つのロールを実ネットワーク上の装置に割当てる。図 3 に示される VPN ポリシーを図 5 の実ネットワーク 100 上に適用する場合に、図 2 または図 8 の経路モデル 200 における第一エンド 211 が図 5 のサーバ A 101 (プロジェクトサーバ) に、図 2 または図 8 の第二エンド 219 が図 5 のグループ FG 109 (プロジェクトに所属する端末) に対応している。したがって、VPN 管理者は、サーバ A 101 に「第一エンド 211」を、グループ FG 109 に「第二エンド 219」を割当てる。これらの割当てられた情報は、経路モデル割当部 13 によって、選択/割当情報記憶部 16 に格納される (ステップ S 5)。

【0053】つぎに、VPN 管理者は、二つのエンドポイント間の経路上に存在するロールを、実ネットワーク上の各装置に割当てる処理を行う。割当てにあたって、最小数が 1 すなわち必須となっているロールから順に割当を行う (ステップ S 6)。この際、VPN 管理者は、図 6 に示される実ネットワーク上に存在する装置の構成情報を参照しながら割当を行う。

【0054】図 2 の経路モデルでは、第一 VPN 213 および第二 VPN 217 が必須のロールであるので、まず、これらの第一 VPN 213 および第二 VPN 217 について割当てを行う。図 5 および図 6 より、サイト A、B のどちらにも IPsec 機能を有する装置が一つしかなく、そのいずれもが各エンドノード (エンドポイント) とインターネットの中間に位置するという構成条件を満たすので、経路モデル割当部 13 は、サイト A の VPN 装置 C 103 にロール「第一 VPN 213」を、サイト B の VPN 装置 E 105 にロール「第二 VPN 217」を割当てる。そして、割当てられた結果は、選択/割当情報記憶部 16 に格納される。

【0055】その後、最小数が0であるルールを順に割当て、その結果を選択／割当情報記憶部16に格納する(ステップS7)。図5および図6より、サイトB間のファイアウォール装置D104はパケットフィルタリング機能を有し、第二VPN217に対応するVPN装置E105とインターネットとの中間に位置しているの
で、ルール「第二外部ファイアウォール216」の適用条件を満たしている。したがって、経路モデル割当部13は、VPN管理者からの指示により、ファイアウォール装置D104にルール「第二外部ファイアウォール216」を割当てる。

【0056】一方、図2または図8の経路モデル200中の「第一外部ファイアウォール214」というルールは、パケットフィルタリング機能を有し、第一エンド211よりもインターネットの側に位置する条件を有するものであるが、図5および図6より、実ネットワーク100上にはこれに対応する装置が存在しない。また、最小数が“0”であるので、この「第一外部ファイアウォール214」というルールは必須ではない。したがって、図2のルール「第一外部ファイアウォール214」は、図5の実ネットワーク100上の装置には割当てられない。同様に、図2または図8に示される経路モデル200中の他のルール「第一内部ファイアウォール212」および「第二内部ファイアウォール218」を満たす装置も、図5の実ネットワーク100上の装置には存在しないので、これらのルールは割当てられない。このように、すべてのルールについて割当てを行った後に、経路モデル割当部13によるルールの割当作業は終了する。

【0057】図9は、経路モデル割当部13によって割当てられた実ネットワーク100上の装置と経路モデル200のルールとの対応関係を示す図である。図9中の点線301~305が、実ネットワーク100内の装置と割当てたルールとの対応関係を示している。上述したように経路モデル200への割当ての結果、サーバA101に第一エンド211のルールが、グループFG109に第二エンド219のルールが、VPN装置C103に第一VPN213のルールが、VPN装置E105に第二VPN217のルールが、そしてファイアウォール装置D104に第二外部ファイアウォール216のルールが、それぞれ割当てられることになる。そして、これらの割当て結果は、上述したように選択／割当情報記憶部16に格納されている。

【0058】つぎに、設定データ生成部14は、これらの割当結果と、ネットワーク装置構成情報格納部6に格納されている装置の構成情報と、VPNポリシーとを用いて、割当てられたこれらの個々の装置に対して設定データを生成する(ステップS8)。すなわち、これらの割当てられた装置のそれぞれに対して、図3に示されるVPNポリシーが適用されるように設定される。こ

で、設定データ生成部14は、VPNポリシーに含まれるルールの部分に、割当結果である実ネットワーク100上の装置の構成情報を代入する処理を行う。具体的には、VPNポリシーに含まれるルールの部分に、実ネットワーク100上の装置の構成情報に含まれるIPアドレスが代入される。なお、ネットワーク装置構成情報格納部6が無い場合やネットワーク装置構成情報格納部6に該当する構成情報が入力されていない場合には、ここで管理用入出力部2よりそれぞれの装置の構成情報を入力してもよい。このようにして、各装置に適用されるVPNポリシーが生成される。

【0059】図10は、この処理の結果として生成された設定データを表す図である。この図は、図3に示されるVPNポリシーのパラメータとしてルール名が入力されている部分に、実ネットワーク上のIPアドレスが入力され、不要の装置についてのルールを削除したものである。そして、この設定データは、設定データ生成部14によって選択／割当情報記憶部16に格納される。

【0060】その後、設定部15は、選択／割当情報記憶部16に格納された設定データにしたがって、実ネットワーク上の各装置に対して設定を行う(ステップS9)。設定部15は、ネットワークなどの接続線21を介して実ネットワーク上の各装置と接続されており、設定情報を各装置に送信し、設定することができる。そして、VPNを構築しようとする実ネットワーク上の装置に対するVPNポリシーの設定が終了する。

【0061】以上説明したように、この実施の形態1によれば、装置の備えるべき機能で表現されたルール列からなる経路モデルと、該経路モデルを構成する各ルールに対して定義されたVPNポリシーに基づいて、設定経路上にVPNポリシーを設定するようにしたので、設定経路上の装置にVPNポリシーを割当てただけで、各装置に対する設定データを生成することができる。また、VPNポリシーには、各装置間の関係が関連付けされているので、VPNの構築を容易にすることができる。そして、それまで装置ごとに行っていた設定作業を、一つの経路を単位として行う設定作業とすることができ、VPN構築の作業時におけるVPN管理者の作業負担を軽減することができるという効果を奏する。

【0062】実施の形態2。図11は、この発明にかかるVPNポリシー管理装置の実施の形態2を示すブロック図である。この図11において、実施の形態1と異なる箇所は、ネットワーク装置構成情報格納部6に、実ネットワーク上の装置の配置構成を示す情報についても格納される点、および経路モデル割当部13がツリー構造生成機能13aとルール割当機能13bとを有するように構成されている点である。その他の構成要素であって上述した実施の形態1と同一の構成要素には、同一の符号を付してその説明を省略している。

【0063】ネットワーク装置構成情報格納部6には、

10

20

30

40

50

VPNを構築しようとしている実ネットワーク上の設定経路上における他の装置との配置関係がさらに格納される。図12は、ネットワーク装置構成情報格納部6に格納される設定経路上の各装置の構成情報およびセグメント情報の一例を示す図である。また、図13は図12に格納されている各装置の構成情報およびセグメント情報の基となるVPNを構築しようとしている設定経路の模式図を示すものである。

【0064】図12(A)に示される設定経路上の装置の構成情報は、図6に示される構成情報に加えて、各装置間の配置位置が規定される項目としての「保有インタフェース」が設けられている。この保有インタフェースには、隣接する装置との間のインタフェース名が格納される。また、図12(B)は、ネットワーク装置構成情報格納部6に上述した(A)の構成情報とは別に格納されるセグメント情報の一例を示す図である。このセグメント情報には、各装置間を接続する「セグメント名」とその「接続インタフェース」が格納される。ここで、図13に示されるように各装置とインターネット側のセグメントとのインタフェースは、各装置の英数字に「1」を付して表し、それとは反対側の各装置とセグメントとのインタフェースは、各装置の英数字に「2」を付して表している。例えば、図13において、VPN装置C403は、インタフェースC1とC2の二つのインタフェースを有し、そのうちインタフェースC1はインターネット側のセグメント1と接続され、インタフェースC2はエンドポイント側のセグメント2と接続される。

【0065】また、ツリー構造生成機能13aは、ネットワーク装置構成情報格納部6に格納されている設定経路上の装置からツリーを生成する機能を有し、ロール割当機能13bは、ツリー構造生成機能13aによって生成されたツリーから経路モデルに適合するエンドポイント間の経路を選択し、該経路上の装置にロールを割当てる機能を有する。

【0066】つぎに、VPNポリシー管理装置1によって、エンドポイント間の装置を自動検出する動作処理手順について図14を参照しながら説明する。図15は、図13に示される設定経路を有する装置同士の隣接関係をツリー表示した図である。なお、この実施の形態2での経路モデルおよびVPNポリシーは上述した実施の形態1で使用した図2および図3を用いるものとする。

【0067】まず、VPN管理者によって、管理用入力部2から図13に示されるサーバAおよびホストF407とホストG408からなるグループFG410との間に、VPNを構築しようとしている設定経路が設定される(ステップS11)。この設定においては、VPN管理者は、ネットワーク装置構成情報格納部6より設定経路上に存在する装置を選択し、さらに該装置の配置情報を管理用入力部2より入力する。ここで入力される配置情報は、図12(A)の構成情報中の「保有インタフェ

ース」および(B)のセグメント情報である。

【0068】つぎに、実施の形態1の図7で説明したステップS1～S5と同じ処理を行って、設定経路上の装置に経路モデル上のエンドロールを割当てる(ステップS12～S16)。すなわち、経路モデルと該経路モデルに対応するVPNポリシーを選択した後に、設定経路上のサーバA401に図2に例示される経路モデルの第一エンドを、グループFG410に同じく第二エンドを割当て、選択/割当情報記憶部16に格納する。

10 【0069】その後、経路モデル割当部13のツリー構造生成機能13aによって、ステップS11で入力された設定経路から図15に示されるツリー構造が生成される(ステップS17)。ここで、このツリー構造を生成するための動作処理手順を図16に示すフローチャートを参照しながら説明する。

20 【0070】まず、経路モデル割当部13のツリー構造生成機能13aは、VPN管理者によって入力された設定経路から、インターネットなどの信頼性の低いネットワークをルートとして設定する(ステップS21)。そして、設定したルートを最初の処理中のノードとし(ステップS22)、該処理中のノードからエンドポイント方向に隣接して接続される装置またはセグメントを該ノードの子ノードとして、幅優先で配置する(ステップS23)。

30 【0071】ツリー構造生成機能13aは、子ノードとして配置されたノードを、つぎに処理中のノードとして設定する(ステップS24)。そして、該処理中のノードに子ノードに対応する装置またはセグメントが存在するか否かを判断する(ステップS25)。ここで、子ノードに対応する装置またはセグメントとは、処理中のノードにエンドポイント方向に隣接して接続される装置またはセグメントのことをいう。もし、処理中のノードに子ノードに対応する装置またはセグメントが存在しないと判断された場合(ステップS25でNoの場合)には、その経路でのツリーの展開処理は該ノードで終了する。これに対して、もし、処理中のノードに子ノードに対応する装置またはセグメントが存在する場合(ステップS25でYesの場合)には、該子ノードに対応する装置またはセグメントが、ツリー全体で既に存在しているか否かを判断する(ステップS26)。子ノードに対応する装置またはセグメントが、ツリー全体で存在していないと判断された場合(ステップS26でNoの場合)には、該装置またはセグメントを処理中のノードの子ノードとして配置する(ステップS27)。その後、ステップS24に戻って、ツリー構造生成機能13aによって、上述した工程が繰り返し実行される。

50 【0072】一方、ステップS26において、子ノードに対応する装置またはセグメントが、ツリー全体で既に存在していると判断された場合(ステップS26でYesの場合)には、既に存在しているその装置またはセグ

メントに対応するノードが、処理中のノードが展開している経路中に存在するの否かについて判断を行う（ステップ S 28）。もし、既に存在している装置またはセグメントに対応するノードが現在展開している経路中に存在するのであれば（ステップ S 28 で Yes の場合）、子ノードに対応する装置またはセグメントの配置処理は行われず（ステップ S 29）、その経路でのツリーの展開処理が終了する。これに対して、もし、既に存在しているノードが現在展開している経路中に存在していないのであれば（ステップ S 28 で No の場合）、子ノードに対応する装置またはセグメントを処理中のノードの子ノードとして配置する処理を行い（ステップ S 30）、その経路でのツリーの展開処理は該配置したノードで終了する。このようにして全ての経路の展開が中止すると、すべての処理は終了する。

【0073】このようにツリー構造生成機能 13a によって、図 15 に示されるツリーが図 13 に示される設定経路から生成される。そして、生成されたツリーにおいて、任意の二つのノード間の経路は、実際のネットワーク上での経路と一致するものとなる。

【0074】再び図 14 に戻り、経路モデル割当部 13 のロール割当機能 13b は、ツリー構造生成機能 13a によって生成されたツリー上のノードに経路モデルのロールを割当てる処理を行う（ステップ S 18）。

【0075】ロール割当機能 13b は、VPN 管理者によって設定されたエンドポイント間の経路を、図 15 に示されるツリーから求める。この例の場合には、つぎの二つの場合が存在することがわかる。経路（A）サーバ A401-セグメント 2-VPN 装置 C403-セグメント 1-インターネット 411-セグメント 3-ルータ I404-セグメント 4-ファイアウォール装置 D405-セグメント 5-グループ FG410 経路（B）サーバ A401-セグメント 2-VPN 装置 C403-セグメント 1-インターネット 411-セグメント 3-ルータ I404-セグメント 4-VPN 装置 E406-セグメント 5-グループ FG410

【0076】つぎに、ロール割当機能 13b は、割当ての必須なロールである第一 VPN および第二 VPN の割当てを行う。第一 VPN および第二 VPN には IPsec 機能が必要であり、またそれはインターネットと第一エンドまたは第二エンドとの中間に配置される必要がある。しかし、上記（A）の経路には、IPsec 機能を有する第二 VPN に該当する装置が存在しないことがわかる。これに対して、（B）の経路では、VPN 装置 C403 に第一 VPN を、VPN 装置 E406 に第二 VPN をそれぞれ割当てることができる。したがって、ロール割当機能 13b は、第一エンドと第二エンドとの間を結ぶ経路として、（B）の経路を選択する。

【0077】そして、ロール割当機能 13b は、選択された（B）の経路のうち、図 2 に示される経路モデル中

他のロールの機能および構成条件、具体的には、最小数が“0”であるロールの機能および構成条件を満たす装置を求める。この図 13 および図 15 に示される例では、最小数が“0”のロールとして、第一外部ファイアウォール、第二外部ファイアウォール、第一内部ファイアウォールおよび第二内部ファイアウォールがあるが、これらのロールの機能条件と構成条件の両者を満足する装置は（B）の経路上には存在しない。したがって、ロール割当機能 13b は、これらの最小数が“0”であるロールを割当てる装置が存在しないと判断し、これらの割当処理を行わない。これらの割当結果は、選択／割当情報記憶部 16 に格納される。このようにしてすべてのロールに対して割当処理が行われた後に、設定経路上の装置の検出が終了する。

【0078】その後、設定データ生成部 14 は、これらの割当結果と、ネットワーク装置構成情報格納部 6 に格納されている構成情報と、VPN ポリシーとを用いて、これらの個々の装置に対して設定データを生成し、選択／割当情報記憶部 16 に格納する（ステップ S 19）。

そして、設定部 15 は、選択／割当情報記憶部 16 に格納された設定データにしたがって、接続線 21 を介して接続された設定経路上の各装置に対して設定を行う（ステップ S 20）。そして、VPN を構築しようとする実ネットワーク上の装置に対する VPN ポリシーの設定が終了する。

【0079】以上説明したように、この実施の形態 2 によれば、インターネットをルートとした隣接関係のツリーを生成し、ツリーのエンドノードに経路モデルのエンドロールを割当てることによって、エンドノード間の経路を自動的に求めることが可能となる。そして、この方法によって、VPN 管理者は、VPN を張りたいエンドポイントを指定することにより、エンドポイント間に存在する装置構成を意識することなく VPN を構築できるようになり、VPN 管理の作業効率がさらに向上する。

【0080】

【発明の効果】以上説明したように、この発明によれば、VPN を構築するために必要な機能で表現した複数のロールからなる経路モデルと、前記経路モデルに対応して作成され、該経路モデルを構成する各ロールに対して定義される一部に他のロールをパラメータとして含む VPN ポリシーとを備え、設定経路上の二つのエンドポイントに経路モデルの終端部を定義するエンドロールが割当てられると、経路モデルのロールを設定経路上の装置に割当てて、VPN ポリシーから設定データを生成する VPN 構築手段とを備えるように構成したので、VPN を構築する設定経路上の各装置間の関係が関連付けられ、VPN の構築を容易にすることができる。また、VPN の構築にあたって、設定作業を装置ごとではなく、一つの経路を単位として行うことができ、VPN 管理者の作業負担を軽減することができるという効果を奏す

る。

【0081】 つぎの発明によれば、設定経路中に存在する装置またはセグメントの接続関係を、インターネットをノードとしたツリー構造を生成し、該ツリー構造を用いて設定経路上の装置に経路モデルのロールを割当てるように構成したので、VPN管理者は、VPNを張りたいエンドポイントを指定するだけで、エンドポイント間に存在する装置構成を意識することなくVPNを構築できるようになり、VPN管理の作業効率がさらに向上するという効果を奏する。

【0082】 つぎの発明によれば、経路モデルが、必要とする機能条件、前記設定経路上での位置が規定される構成条件、および経路モデル中で必要とされる数によって定義された、複数のロールによって構成されているので、装置に依存しない汎用性の高い設定条件を提供することができるという効果を奏する。また、同じような構成のVPNを構築する際において、経路モデルを備えることにより、VPNを構築するたびに装置の動作処理条件を設定しなくてすむので、VPN管理者の作業効率を向上させることができるという効果も奏する。

【図面の簡単な説明】

【図1】 この発明の実施の形態1のVPNポリシー管理装置の構成を示すブロック図である。

【図2】 経路モデルの一例を示す図である。

【図3】 図2の経路モデルに対応するVPNポリシーの一例を示す図である（その1）。

【図4】 図2の経路モデルに対応するVPNポリシーの一例を示す図である（その2）。

【図5】 VPNを構築しようとしている実際のネットワーク上の経路の一例を示す図である。

【図6】 図5の実際のネットワーク上の経路を構成する装置の構成情報の一例を示す図である。

【図7】 VPN構築の処理手順を示すフローチャート*

*である。

【図8】 図2の経路モデルのロール名を構成条件にしたがって配列した図である。

【図9】 図5の実際のネットワーク上の経路と、図8の経路モデルとの対応関係を示す図である。

【図10】 VPN構築手段によって生成された設定データの一例を示す図である。

【図11】 この発明の実施の形態2のVPNポリシー管理装置の構成を示すブロック図である。

10 【図12】 ネットワーク装置構成情報格納部に格納されている装置の構成情報の一例を示す図であり、(A)は装置の構成情報を、(B)はセグメント情報を示している。

【図13】 この発明の実施の形態2を説明するための実際のネットワーク上の経路の一例を示す図である。

【図14】 VPN構築の処理手順を示すフローチャートである。

【図15】 実施の形態2の方法によって、図13のネットワーク構成をツリー表示した図である。

20 【図16】 設定経路からツリー構造を生成する処理手順を示すフローチャートである。

【図17】 従来のVPNの構成を示す図である。

【図18】 従来のVPNの構成を示す図である。

【図19】 従来のVPNの構成を示す図である。

【符号の説明】

1 VPNポリシー管理装置、2 管理用入出力部、3 VPN構築手段、4 経路モデル定義格納部、5 VPNポリシー定義格納部、6 ネットワーク装置構成情報格納部、11 経路モデル選択部、12 VPNポリシー選択部、13 経路モデル割当部、13a ツリー構造生成機能、13b ロール割当機能、14 設定データ生成部、15 設定部、16 選択／割当情報記憶部、20 装置、21 接続線。

【図2】

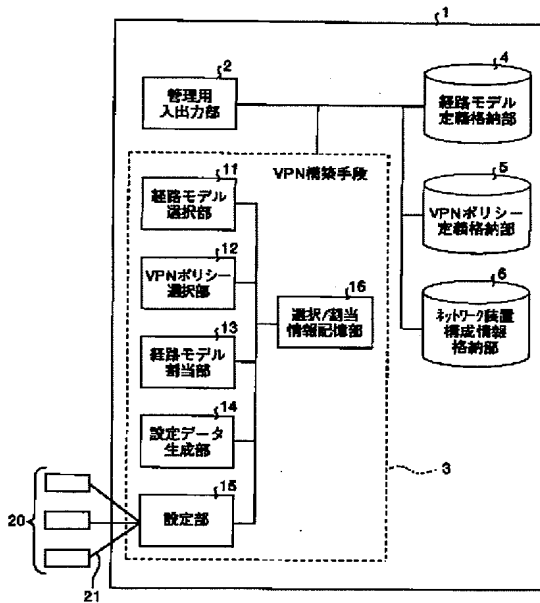
経路モデル名：サイト間VPN経路モデル

ロール名	機能条件	構成条件	最小数	最大数
第一エンド	送受信機能	—	1	複数
第二エンド	送受信機能	—	1	複数
第一VPN	IPsec機能	インターネット<第一VPN≤第一エンド	1	1
第二VPN	IPsec機能	インターネット<第二VPN≤第二エンド	1	1
第一外部FW	PF機能	インターネット<第一外部FW<第一VPN	0	複数
第二外部FW	PF機能	インターネット<第二外部FW<第二VPN	0	複数
第一内部FW	PF機能	第一VPN<第一内部FW<第一エンド	0	複数
第二内部FW	PF機能	第二VPN<第二内部FW<第二エンド	0	複数

FW：ファイアウォール

PF：パケットフィルタリング

【図1】



【図4】

設定先ロール	規則	
	条件	アクション
第二VPN	方向=out Src=第一エンド Dst=第二エンド Service=telnet (開始)	Action=暗号 対向装置=第一VPN Proposal=ABC
	方向=in Src=第二エンド Dst=第一エンド Service=telnet	Action=暗号 対向装置=第二VPN Proposal=ABC
第二外部FW	方向=out Src=第二VPN Dst=第一VPN Service=IKE	Action=通過
	方向=out Src=第二VPN Dst=第一VPN Service=IPsec	Action=通過
	方向=in Src=第一VPN Dst=第二VPN Service=IKE	Action=通過
	方向=in Src=第二VPN Dst=第一VPN Service=IPsec	Action=通過
第二内部FW	方向=out Src=第二エンド Dst=第一エンド Service=telnet (開始)	Action=通過
	方向=in Src=第一エンド Dst=第二エンド Service=telnet	Action=通過

FW: ファイアウォール Src: 発信元 Dst: 発信先

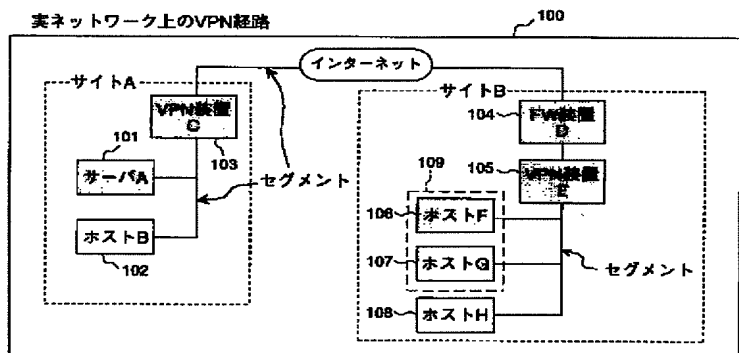
【図3】

VPNポリシー名: プロジェクトサーバポリシー
VPNポリシー

設定先ロール	規則	
	条件	アクション
第一VPN	方向=out Src=第一エンド Dst=第二エンド Service=telnet	Action=暗号 対向装置=第二VPN Proposal=ABC
	方向=in Src=第二エンド Dst=第一エンド Service=telnet (開始)	Action=暗号 対向装置=第一VPN Proposal=ABC
第一外部FW	方向=out Src=第一VPN Dst=第二VPN Service=IKE	Action=通過
	方向=out Src=第一VPN Dst=第二VPN Service=IPsec	Action=通過
	方向=in Src=第二VPN Dst=第一VPN Service=IKE	Action=通過
	方向=in Src=第二VPN Dst=第一VPN Service=IPsec	Action=通過
第一内部FW	方向=out Src=第一エンド Dst=第二エンド Service=telnet	Action=通過
	方向=in Src=第二エンド Dst=第一エンド Service=telnet (開始)	Action=通過

FW: ファイアウォール Src: 発信元 Dst: 発信先

【図5】

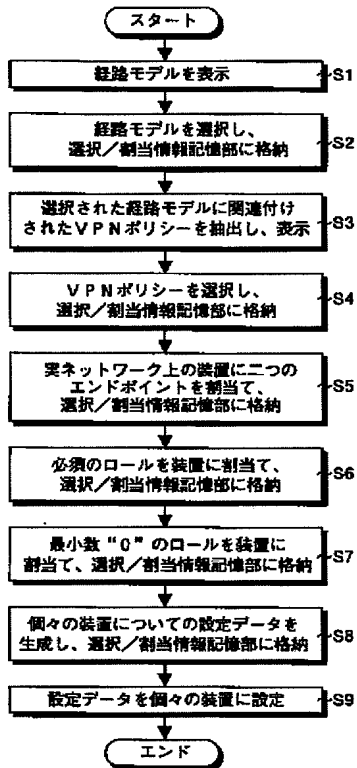


【図6】

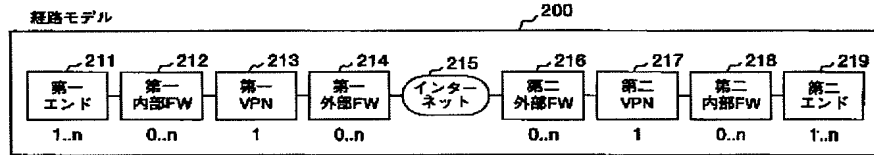
装置名	IPアドレス	機能
サーバA	133.141.10.2	送信機能、受信機能
ホストB	133.141.10.3	送信機能、受信機能
VPN装置C	133.141.10.1	パケットフィルタリング機能 IPsec機能
FW装置D	200.74.1.1	パケットフィルタリング機能
VPN装置E	200.74.8.1	IPsec機能
ホストF	200.74.8.101	送信機能、受信機能
ホストG	200.74.8.102	送信機能、受信機能
ホストH	200.74.8.103	送信機能、受信機能

FW: ファイアウォール

【図7】



【図8】

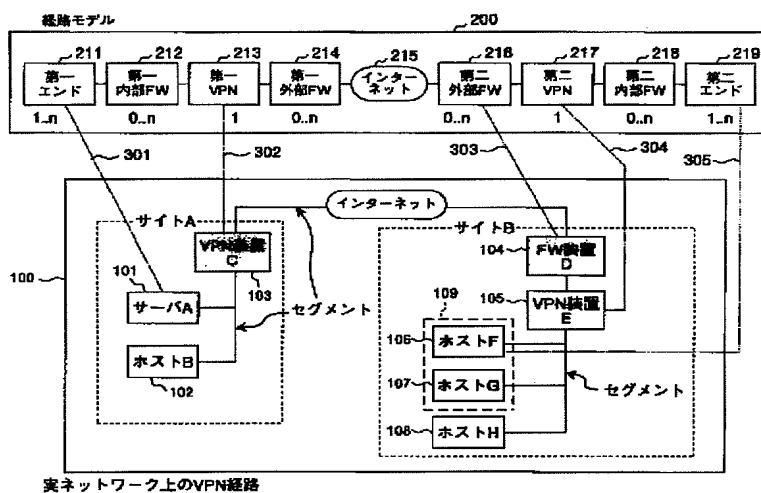


【図10】

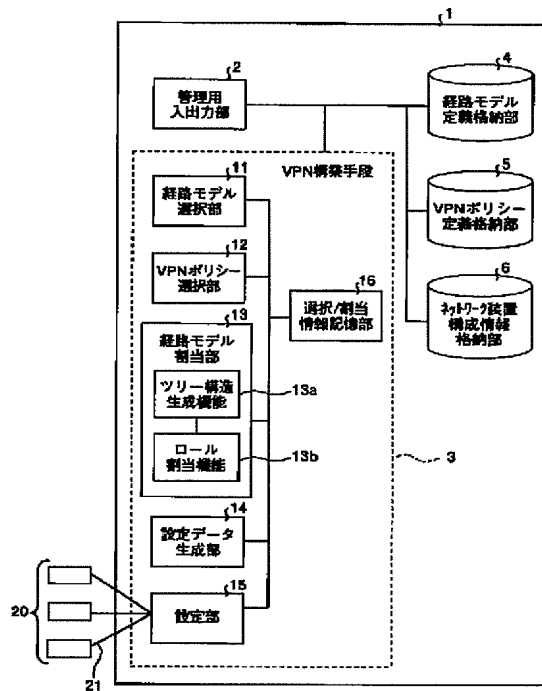
設定先ルール	規則	
	条件	アクション
第一VPN	方向=out Srcアドレス=133.141.10.2 Dstアドレス=200.74.8.101~200.74.8.102 Service=telnet	Action=暗号 対向装置=200.74.8.1 Proposal=ABC
	方向=in Src=200.74.8.101~200.74.8.102 Dst=133.141.10.2 Service=telnet (開始)	Action=暗号 対向装置=200.74.8.1 Proposal=ABC
第二VPN	方向=out Src=200.74.8.101~200.74.8.102 Dst=133.141.10.2 Service=telnet	Action=暗号 対向装置=133.141.10.1 Proposal=ABC
	方向=in Src=133.141.10.2 Dst=200.74.8.101~200.74.8.102 Service=telnet	Action=暗号 対向装置=133.141.10.1 Proposal=ABC
第二外部FW	方向=out Src=200.74.8.1 Dst=133.141.10.1 Service=IKE	Action=通過
	方向=out Src=200.74.8.1 Dst=133.141.10.1 Service=ESP	Action=通過
	方向=in Src=133.141.10.1 Dst=200.74.8.1 Service=IKE	Action=通過
	方向=in Src=133.141.10.1 Dst=200.74.8.1 Service=ESP	Action=通過

FW: ファイアウォール Src: 発信元 Dst: 発信先

【図9】



【図11】



【図12】

装置構成情報

装置名	IPアドレス	機能	保有インタフェース
サーバA	133.141.10.2	送信機能、受信機能	C1,C2
ホストB	133.141.10.3	送信機能、受信機能	A1
VPN装置C	133.141.10.1	パケットフィルタリング機能 IPsec機能	I1, I2, I3
ルータI	200.74.1.0	ルーティング機能	B1
FW装置D	200.74.1.1	パケットフィルタリング機能	D1,D2
VPN装置E	200.74.8.1	IPsec機能	E1,E2
ホストF	200.74.8.101	送信機能、受信機能	F1
ホストG	200.74.8.102	送信機能、受信機能	G1
ホストH	200.74.8.103	送信機能、受信機能	H1

FW：ファイアウォール

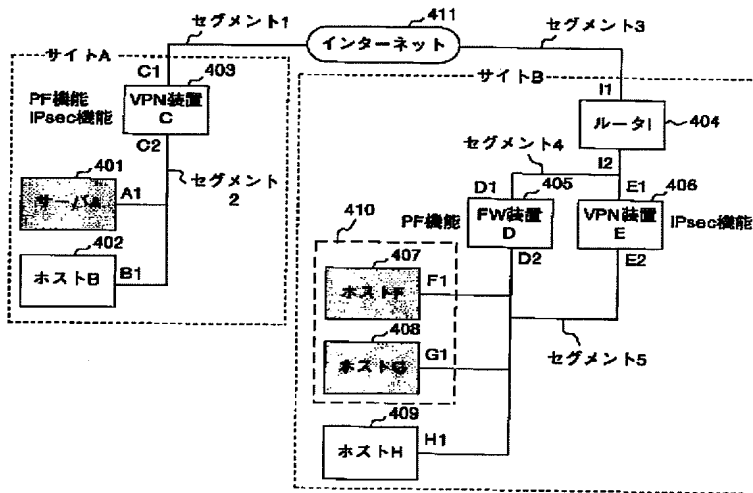
(A)

セグメント情報

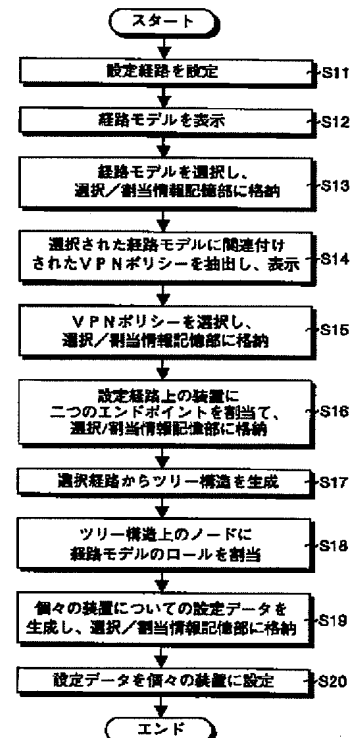
セグメント名	接続インタフェース
セグメント1	C1, (インターネット)
セグメント2	C2, A1, B1
セグメント3	I1, (インターネット)
セグメント4	I2, D1, E1
セグメント5	D2, E2, F1, G1, H1

(B)

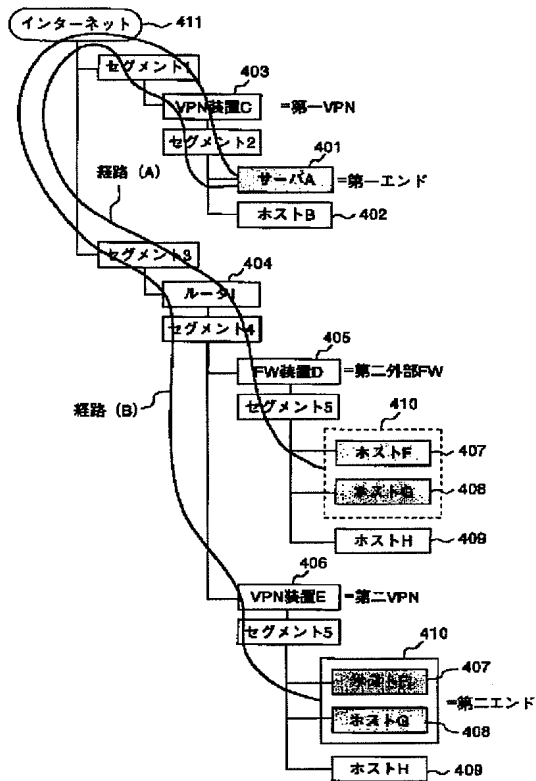
【図13】



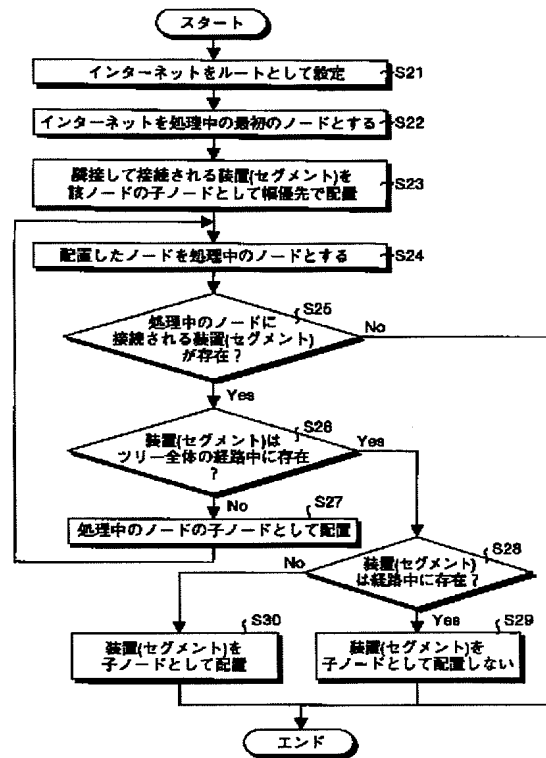
【図14】



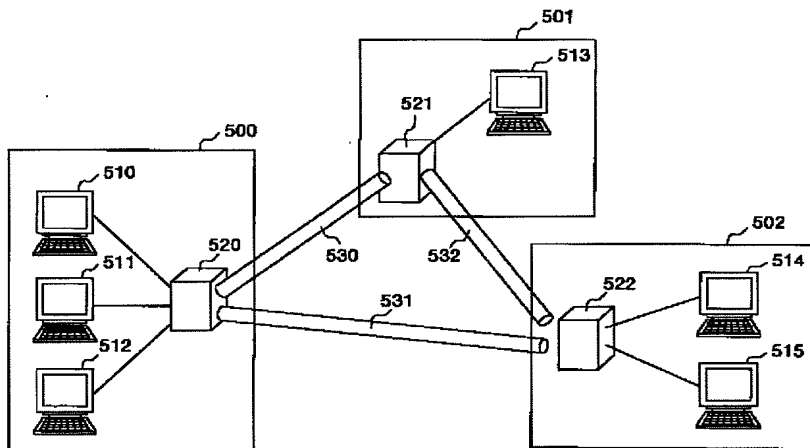
【図15】



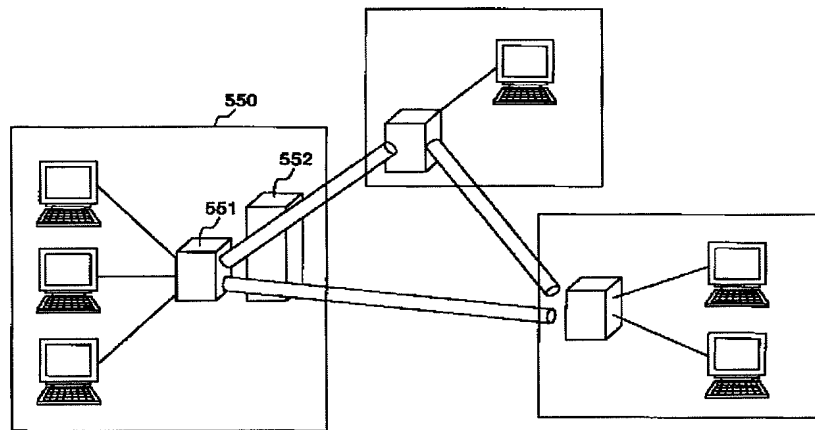
【図16】



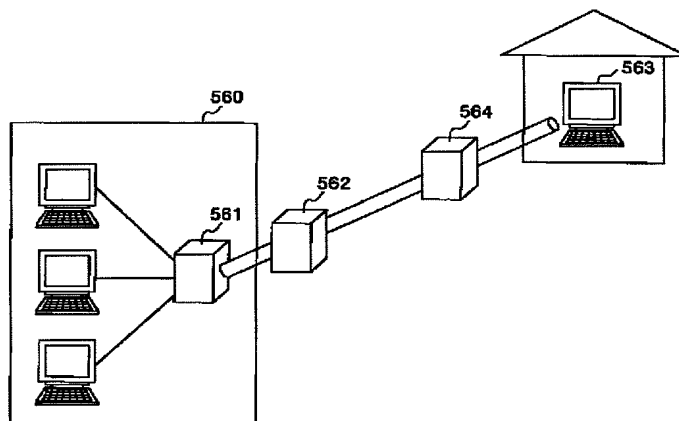
【図17】



【図18】



【図19】



フロントページの続き

(72)発明者 高野 啓
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72)発明者 金枝上 敦史
東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

Fターム(参考) 5K030 GA15 GA17 HA08 HC01 JA10
KA07 LB05 MD04 MD06